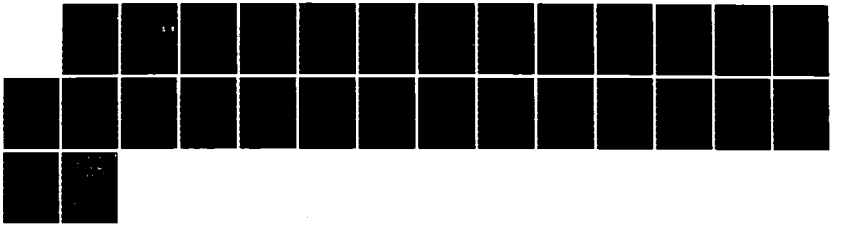
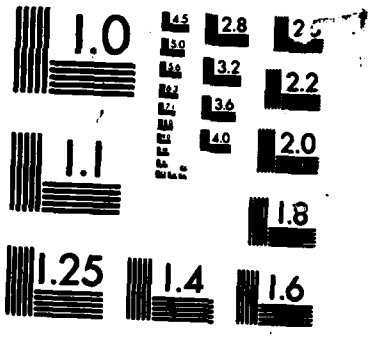
AD-A166 430 USER'S MANUAL FOR THE SECURE MILITARY MESSAGE SYSTEM M2 1/1
PROTOTYPE(U) NAVAL RESEARCH LAB WASHINGTON DC
B T TRETICK ET AL. 28 MAR 86 NRL-MR-5757

UNCLASSIFIED F/G 17/2 NL





NRL Memorandum Report 5757

User's Manual for the Secure Military Message System M2 Prototype

B. T. TRETICK, M. R. CORNWELL, C. E. LANDWEHR,
R. J. K. JACOB AND J. M. TSCHOHL

Computer Science and Systems Branch
Information Technology Division

March 28, 1986

NAVAL RESEARCH LABORATORY
Washington, D.C.

SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

1a. REPORT SECURITY CLASSIFICATION UNCLASSIFIED	1b. RESTRICTIVE MARKINGS
2a. SECURITY CLASSIFICATION AUTHORITY	3. DISTRIBUTION / AVAILABILITY OF REPORT Approved for public release; distribution unlimited.
2b. DECLASSIFICATION / DOWNGRADING SCHEDULE	
4. PERFORMING ORGANIZATION REPORT NUMBER(S) NRL Memorandum Report 5757	5. MONITORING ORGANIZATION REPORT NUMBER(S)
6a. NAME OF PERFORMING ORGANIZATION Naval Research Laboratory 6b. OFFICE SYMBOL (If applicable) Code 7593	7a. NAME OF MONITORING ORGANIZATION
6c. ADDRESS (City, State, and ZIP Code) Washington, DC 20375-5000	7b. ADDRESS (City, State, and ZIP Code)
8a. NAME OF FUNDING/SPONSORING ORGANIZATION Naval Surface Weapons Sys. Center 8b. OFFICE SYMBOL (If applicable) Code 8144	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
8c. ADDRESS (City, State, and ZIP Code) Washington, DC 20363-5001	10. SOURCE OF FUNDING NUMBERS PROGRAM ELEMENT NO: O&MN PROJECT NO: TASK NO: WORK UNIT ACCESSION NO: DN880-204

11. TITLE (Include Security Classification)
User's Manual for the Secure Military Message System M2 Prototype

12. PERSONAL AUTHOR(S)
Tretick, B. T., Cornwell, M. R., Landwehr, C. E., Jacob, R. J. K. and Tschohl, J. M.

13a. TYPE OF REPORT	13b. TIME COVERED	14. DATE OF REPORT (Year, Month, Day)	15. PAGE COUNT
Interim	FROM 6/85 TO 8/85	1986 March 28	28

16. SUPPLEMENTARY NOTATION

17. COSATI CODES		
FIELD	GROUP	SUB-GROUP

18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
Message systems ; User documentation
Computer security ;

19. ABSTRACT (Continue on reverse if necessary and identify by block number)

This manual describes the M2 prototype of the Secure Military Message System (MMS). It is organized in two parts: the User's Guide and the Reference Manual. The User's Guide includes a discussion of how one performs various tasks using the MMS, followed by a sample session. The Reference Manual is provided for the more experienced user. It supplies tables and guides for quick reference.

20. DISTRIBUTION / AVAILABILITY OF ABSTRACT ☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT ☐ DTIC USERS	21. ABSTRACT SECURITY CLASSIFICATION UNCLASSIFIED
22a. NAME OF RESPONSIBLE INDIVIDUAL Mark R. Cornwell	22b. TELEPHONE (Include Area Code) (202) 767-3365 22c. OFFICE SYMBOL Code 7596

DD FORM 1473, 84 MAR 83 APR edition may be used until exhausted
All other editions are obsolete

SECURITY CLASSIFICATION OF THIS PAGE

CONTENTS

PART I: USER'S GUIDE

INTRODUCTION 1

BASIC CONCEPTS 1

USING THE MMS 2

Login and Logout 2
Reading and Filing Mail 2
Composing Messages 3
Sending and Forwarding Messages 3
Text Files 3
Permissions 3
Further Details 4

A SHORT SCENARIO 5

PART II: REFERENCE MANUAL

A LIST OF COMMANDS BY MENU 9

FUNCTION KEY OVERLAYS 12

EDITOR COMMANDS 13

ERROR MESSAGES 14

KEY WORDS AND ABBREVIATIONS 19

APPENDIX A — The Secure MMS M2 Prototype Tourguide 21

APPENDIX B — NRL Secure Military Message System Project Bibliography 23

USER'S MANUAL FOR THE SECURE MILITARY MESSAGE SYSTEM M2 PROTOTYPE

Part I: User's Guide

Introduction

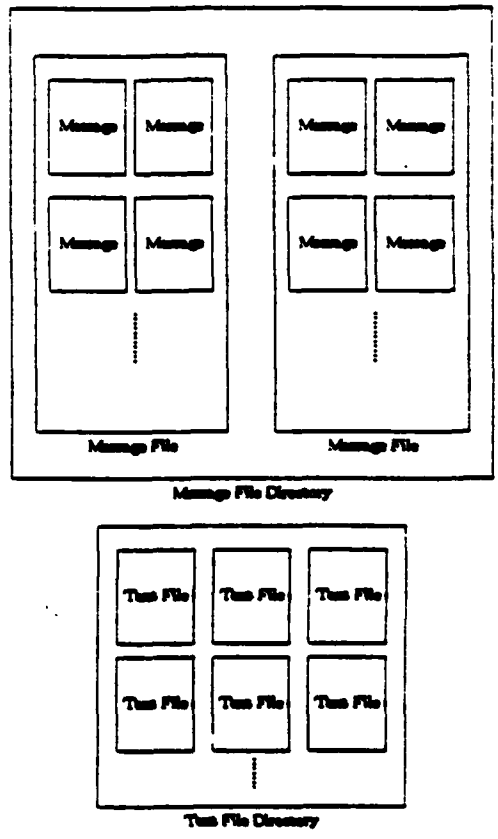
The Secure Military Message System (MMS) supports composition, transmission, receipt, and filing of military messages. It is designed to control the access that users with different clearances have to messages of different classifications. Security markings are maintained on messages and message fields, and operations are permitted only if they are consistent with the MMS security model.

This manual is organized in two parts: the User's Guide and the Reference Manual. The User's Guide includes a discussion of how one performs various tasks using the MMS, followed by a sample session. It does not cover all details of MMS operations; in particular, security officer functions are omitted. The Reference Manual is provided for the more experienced user. It supplies tables and guides for quick reference.

Basic Concepts

The electronic world of the system provides analogs for familiar objects in the physical world. There are three concepts basic to the system: the entity hierarchy, the electronic mail functions, and the security enforcement.

The MMS provides an environment for file management similar to that of a physical file cabinet. A file cabinet contains drawers, which in turn contain the files of messages and documents. In the MMS, you will have your own *message file directory* analogous to the file cabinet. The message file directory contains *message files* that in turn contain the *messages*. You will also have a *text file directory* that contains *text files*. The following diagram illustrates that arrangement.



Messages are sent and received in a way similar to conventional mail systems. The *send* operation places the message in each recipient's *inbox*, the system's version of the mailbox. The recipient can then read, store, and (if permitted) forward the message to others.

A message is either *formal* or *informal*. Informal messages can be sent by any user. Formal messages correspond to military communications of record. They are usually sent between commands rather than individuals, and they can only be sent by designated individuals, called *releasers*.

Manuscript approved January 17, 1986.

The MMS security model governs what actions the system may perform on your behalf. This model is based on the same policy that controls the handling of classified paper documents. It requires that a classification be associated with each directory, file, and message in the system and that these classifications must be ordered in the MMS entity hierarchy as they would be in the physical world. For example, a Confidential message may only contain fields at that security level or below, a Secret file must only contain messages at that security level or below, and a Top Secret directory must only contain files at that level or below. The MMS protects classified information by checking security *labels* (eg. (T), (S nato)) associated with users and data to determine whether a requested operation is consistent with the policy.

Using the MMS

Login and Logout

During the login sequence, you identify yourself to the MMS by supplying your *userid* and your *password*. Your userid is usually your last name (in lower case), and also serves as your address for receiving messages. Your password should be kept private, so that it is known only by you. The message system accepts it as proof of your identity.

The *screen classification* you choose limits the classification of information displayed on the terminal screen. Only data with a security classification that is less than or equal to that of the screen may be displayed on it. You cannot choose a screen classification higher than your clearance.

Your choice of *roles* determines the operations you can perform with the MMS. Each person is authorized for one or more roles. At login, you select an initial set of roles for the current session. You can change this selection during a session.

The *User* role permits you to perform normal message handling tasks. Other roles are required for some operations; for example, the *Releaser* role is required to send a Formal message, and the *Downgrader* role is required to lower the classification of text files or message files.

When you complete a session with the MMS, you *logout*. The screen is cleared and the terminal is set up for a new login.

Reading and Filing Mail

Displaying your message file directory lists all of your message files and their security classifications. In turn, displaying a message file lists an entry for each message currently in that file. The message entry shows the message's sender, subject, type, and classification. The entry is marked (N) if it is new, and (D) if it has been deleted, and its date-time-group (DTG) is shown. The DTG is a unique identifier for a message, composed of the date and time of its creation and the site where it was created. If a message's classification is greater than the current screen classification, its entry will show only the DTG.

To view a specific message, use the *Display* command, supplying either the file name and message number within the file or by specifying its DTG. A hard copy of the message can be produced with the *Print* command.

The *Create Message File* command adds a new message file to your directory; you designate its name and classification. Sometimes, observing a collection of messages at one security level (say, Confidential) may permit a user to infer more sensitive information (say, Secret). This is called the *aggregation* problem. To help you deal with this problem, the MMS allows you to restrict a message file so that even though another user is cleared to read individual messages in that file, he is not permitted to do so unless his clearance is at least equal to the classification of the file as a whole. To impose this discipline on a message file, it must be designated *Container Clearance Required* (CCR) when it is created. Thus, a file of aggregation-sensitive Confidential messages might properly be created as Secret CCR.

The *Copy* and *Move* commands are used to move messages between files. Copy causes a message to appear in a new file. The two files will share the same message: changing one copy changes the other. Move is like Copy, except that Move deletes the

copy of the message in the file it was moved from. A deleted message can be retrieved with the *Undelete* command. The *Expunge* command removes all deleted messages from the file and destroys them.

Composing Messages

The *Create Message* command invokes the message editor, which displays a skeleton message made up of several *fields*. To compose the message, move the cursor to the desired fields with the arrow keys, and enter the appropriate information. Three of the fields (From, Security, and Originator) appear above a bar on the screen; these fields are unalterable.

The text field of a message has an overall classification (initially set to that of the message), but you must also enter an explicit classification for each paragraph within the text field, including the first. To create a new paragraph, press the *Make New Paragraph* function key. You will be prompted to classify the paragraph before typing the text.

You can correct an error by positioning the cursor just after the error, backspacing over it, and typing the correction, or you may use the function keys. The *Undo* operation undoes the last command you gave, and then prompts you to decide whether you want to undo more.

When you are satisfied with the edited message, select *Finished Editing and Update*. The MMS will then check the syntax, check that the classification of each message field is less than or equal to that of the message as a whole, and report any faults. These must be corrected before the message can be updated.

To end an editing session *without* saving the changes, select *Finished Editing and Abort*. The message will not be updated.

When you *Edit* a message, the message is put back into the message editor, where you can make the necessary changes using the same techniques.

Sending and Forwarding Messages

Send makes a copy of the message appear in the inbox of each recipient, and changes the Draft mark on the message to a Sent mark. Only Draft messages may be sent. To send a Formal message, you must have Releaser as a current role.

Forward delivers a copy of the message to specified addressees with a tag attached, marking the message for Action, Information, Release, or Coordination.

Reply is like Create Message, except that the To and Subject fields are automatically filled in with the From and Subject fields, respectively, of the message to which you are replying.

Send and related commands are located in the *Send Message Menu*, which can be selected by pressing the corresponding function key.

Text Files

A *text file* is a list of paragraphs, like the text field of a message. It can be used to store or edit text fields or other message fields (for example, address lists from To or CC fields) as well. It is composed and edited in the same manner as a text field. Your *text file directory* contains all of your text files, which you refer to by name.

Operations (selected from the *Copy and Duplicate Menu*) are provided for copying message fields into text files and vice versa. When a text file is deleted, it cannot be recovered.

Permissions

By default, none of your messages can be read or edited by anyone else. Sharing a message with others can be accomplished by changing the *permissions* on a particular message.

Each message, message file, text file, and directory has a set of permissions that defines the commands each person can invoke on that entity. Initially, only the owner has any permissions. One of these permissions allows him to edit the permissions of his files to provide others with access to his data. He can, for example, allow another person to read a particular message, or, if he is working jointly on a message, he can grant co-authors editing permissions. The other persons must still have proper clearances to have access to classified data.

The *Show Permits* and *Change Permits* commands are located in the *Security Menu*, which can be selected by pressing the appropriate function key. Show Permits displays the permissions of the specified object on the screen as a table with users along the top and commands down the side. A permission is either yes (%) or no (-). *Print Permits* sends the permission table to the printer.

The *Change Permits* command allows you to edit the table. Use the arrow keys to position the cursor at the appropriate entry, and click the space bar to make the change. If the entry was 'no', it will change to 'yes', and vice versa. When you have finished, either update or abort the edit.

Further Details

The best way to develop an understanding of the MMS is to experiment with it. The following sample session presents the message system pictorially for an introductory walk-through. The Reference Manual contains a listing of other useful commands, describes the editor in more detail, and closes with a bibliography of related MMS project papers.

A Short Scenario

The purpose of this scenario is to provide new users with an idea of how the MMS operates. In this example, a user logs into the message system, reads an incoming message, files it, and composes and sends a reply. We will monitor his progress by means of snap shots of the terminal screen. The screen images will be bounded by lines.

The Login Sequence

To gain access to the MMS, the user (Ben Franklin) must first authenticate his identity to the system by logging in. He does this by supplying his *userid* (franklin) and his *password* (not echoed) to the login prompt. He then selects a *screen classification* (Top Secret white) and a *role* (User).

User:*unidentified* SMMS M2 Prototype Screen:(U)
Login: franklin TOP SECRET white User

Checking login permissions...

The system then checks the login permissions. Upon a valid login, Franklin has access to the message system's resources.

The Inbox

Initially, the screen shows the display of Franklin's *inbox*. Listed here are the *message entries* for messages currently in this *message file*. The message entry shows the message's sender, subject, type, and security classification. Notice that Franklin can not see the message entry for message #1. The reason for this is that the message classification exceeds that of the screen. Commands for the message system that are invoked by pressing the number keys are listed in the menu on the screen. Other commands are issued with the function keys.

User:franklin SMMS M2 Prototype Screen:(T white)

Choose command from menu or from function key overlay

1	2	3	4	5	6	7	8
DISPLAY Msg/File/ Text/Dir	CREATE Msg/File/ Text	DELETE/ UNDEL- -ETE	COPY Msg	MOVE Msg	EXPUNGE File	EDIT Msg/Text	PRINT Msg/File/ Text

Welcome to M2 prototype message system

1 N CC091448AUG75

2 (S white)N CC110412AUG75 Formal Sent
From:(U) ross
Subject:(U) About Ben Arnold

3 (S)N CC131423AUG75 Informal Sent
From:(U) hancock
Subject:(U) Adam's latest excuse

Reading a Message

Franklin can read his mail by using the *Display* command. As a result, the message he choose is displayed on the lower half of the screen, and the system is ready for another command.

User:franklin SMMS M2 Prototype Screen:(T white)

Choose command from menu or from function key overlay

1	2	3	4	5	6	7	8
DISPLAY Msg/File/ Text/Dir	CREATE Msg/File/ Text	DELETE/ UNDEL- -ETE	COPY Msg	MOVE Msg	EXPUNGE File	EDIT Msg/Text	PRINT Msg/File/ Text

Security: (S white)
From: (U) ross
Originator: (U) CC

To: (U) franklin
Cc: (U) adams
Subject: (U) About Ben Arnold
Text: (S white)
(S white) I've been hearing some pretty strange things
around the Olde Inn about Ben Arnold. There's alot of
talk about treason connected to him. George won't
believe me.

(C) Would you talk to him? He listens to you.

Filing a Message

After reading the message, Franklin wishes to file it in his message file named "rumors". He accomplishes this by using the *Move* command. The inbox is updated to show that his message #2 has been marked deleted (D). He now displays his message file rumors, and sees that it has the new message entry.

User:franklin SMMS M2 Prototype Screen:(T white)

Choose command from menu or from function key overlay

1	2	3	4	5	6	7	8
DISPLAY Msg/File/ Text/Dir	CREATE Msg/File/ Text	DELETE/ UNDEL- -ETE	COPY Msg	MOVE Msg	EXPUNGE File	EDIT Msg/Text	PRINT Msg/File/ Text

1 (S white)N CC110412AUG75 Formal Sent
From:(U) ross
Subject:(U) About Ben Arnold

Composing a Message

Now Franklin wants to write a letter to George Washington on the subject of Ben Arnold's behavior. He uses the *Create* command (2) to make an informal message with a security classification of 'SECRET white' in his message file rumors. The message system places him in the message editor, where he simply fills in the various message *fields*, and writes the body of the message in the *Text* field. Notice that the text field has the same classification that he assigned to the message.

Security:(S white)
From:(U) franklin
Originator:(U) CC
Message Classification: S white
To:(U) washington
Cc:(U) ross
Subject:(U) Ben Arnold
Text:(S white)
(S white) Betsy has reinforced my suspicions of Arnold
by bringing to my attention rumors of treason that
are connected to him. I know that rumors can be concocted
by idle minds, but I believe that there is some substance
to these. To my eyes, his behavior warrants close inspection.
(S white) Please consider a formal investigation on this
case - the lives of our countrymen are at stake.

SMMS Message Editor

When the message is complete, he presses the Update key (f8) and the MMS checks the message syntax and security hierarchy. If these checks succeed, the message is written to the file, as shown below.

User:franklin SMMS M2 Prototype Screen:(T white)

Choose command from menu or from function key overlay

1	2	3	4	5	6	7	8
DISPLAY Msg/File/ Text/Dir	CREATE Msg/File/ Text	DELETE/ UNDEL- -ETE	COPY Msg	MOVE Msg	EXPUNGE File	EDIT Msg/Text	PRINT Msg/File/ Text

1 (S white)N CC110412AUG75 Formal Sent
From:(U) ross
Subject:(U) About Ben Arnold

2 (S white)N CC162345AUG75 Informal Draft
From:(U) franklin
Subject:(U) Ben Arnold

Sending a Message

Now that the message is written, Franklin wants to mail it. He selects the *Send Message Menu* from the function key overlay. A new menu appears on the screen.

User:franklin SMMS M2 Prototype Screen:(T white)

Choose command from menu or from function key overlay

1 Send Message	2 Reply to Message	3 Readdress Message	4 Forward Msg for Action	5 Forward Msg for Info	6 Forward Msg for Coord	7 Forward Msg for Release

1 (S white)N CC110412AUG75 Formal Sent
From:(U) ross
Subject:(U) About Ben Arnold

2 (S white)N CC162345AUG75 Informal Draft
From:(U) franklin
Subject:(U) Ben Arnold

He invokes the *Send message* command, and the message is sent to Washington's and Ross's inboxes. The message file is updated to show that the Draft mark on the message has changed to a Sent mark.

Logout

Franklin has finished this session with the MMS and presses the Logout key. The terminal is now ready for a . . login.

Part II: Reference Manual

A List of Commands by Menu

These menus list commands invoked by pressing the number keys on your terminal. The different menus are selected by pressing the corresponding function key.

Main Menu

1	2	3	4	5	6	7	8
DISPLAY Msg/File/ Text/Dir	CREATE Msg/File/ Text	DELETE/ UNDEL- -ETE	COPY Msg	MOVE Msg	EXPUNGE File	EDIT Msg/Text	PRINT Msg/File/ Text

1. *Display* prints a message, text file, message file, or directory on the screen.

2. *Create* is used to compose new messages, text files and message files.

3. *Delete/Undelete* allows the removal of messages, text files, and message files. Deleted messages are marked with a D, and remain in the message file until the file is expunged. Deleted messages can be recovered if they are undeleted before the file is expunged. This is not true with text files or message files — once they are deleted, they are irrevocably destroyed.

4. *Copy Message* makes a duplicate of a message and places it into a target message file. The two messages are tied together - if a change is made in one of them, the other changes also. See also *Duplicate an Object* in the *Copy and Duplicate Menu* .

5. *Move Message* is like *Copy Message*, except that it marks the original message deleted.

6. *Expunge Message File* causes all deleted messages in the specified message file to be irreversibly destroyed. Only prior to an expunge can deleted messages be undeleted.

7. *Edit* allows the user to make changes to messages and text files.

8. *Print* is similar to Display, except that the output is sent to the hard copy printer instead of the screen. The printer marks the security level of the object at the top and bottom of each page.

Send Message Menu

1	2	3	4	5	6	7
Send Message	Reply to Message	Readdress Message	Forward Msg for Action	Forward Msg for Info	Forward Msg for Coord	Forward Msg for Release

1. *Send Message* converts a draft message to a sent message and places a copy of the sent message in each addressee's inbox. Any User may send a draft informal message, but only a person with the Releaser role may send a draft formal message (see Forward for Release).

2. *Reply Message* is similar to *Create Message*, but the Reply function fills in the *To* and *Subject* fields of the message with the *From* and *Subject* fields of the message being replied to.

3. *Readdress Message* makes a draft copy of the specified sent message and allows you to change the address list. Only formal messages can be readdressed.

4. *Forward Message for Action* delivers a copy of the sent message to each person specified in the command and marks each new message entry with 'New' and 'for Action' tags.

5. *Forward Message for Information* delivers a copy of the sent message to each person specified in the command and marks each new message entry with 'New' and 'for Info' tags.

6. *Forward Message for Coordination* delivers a copy of the draft message to each person specified in the command and marks each new message entry with 'New' and 'for Coordination' tags.

7. *Forward Message for Release* delivers a copy of the draft message to a specified person and marks the recipient's message entry with 'New' and 'for Release' tags. The addressees must have the Releaser role. Only draft formal messages can be forwarded for release, and only a Releaser may send a formal message. The addressee may send the message.

Copy and Duplicate Menu

1	2	3	4	5	6
CPY Field to Text by DTG	CPY Field to Text by MF	CPY Text to Field by DTG	CPY Text to Field by MF	CPY Text to Text	Duplicate an object

1. *Copy Field to Text by DTG* appends the specified message field from a message referred to by date-time-group (DTG) to a text file.

2. *Copy Field to Text by MF* appends the specified field in a message referred to by message file and number to a text file.

3. *Copy Text to Field by DTG* copies the contents of a text file to the specified message field in a message referred to by DTG.

4. *Copy Text to Field by MF* copies the contents of a text file to the specified message field in a message referred to by message file and number.

5. *Duplicate an Object* creates a duplicate of a message, text file, or message file. Unlike the Copy command of the Main Menu, the duplicate message is not linked to the original message. A duplicate of a text file is also independent of the original. In the case of a duplicate message file, the messages contained in the original file are copied to the duplicate file. The duplicate messages *are* linked to the original messages, like with the Copy command.

Security Menu

1	2	3	4	5	6	7	8
RECLASS. Text/File/ Term	SHOW Permits	CHANGE Permits	SHOW User Info	CHANGE User Role	CHANGE Password	SHOW Terminal Info	PRINT Permits

1. *Reclassify* allows you to change the classification labels of message files, text files, or the terminal (screen classification). The new classification must still dominate that of the contents of the reclassified entity. You may raise or lower the screen classification, but unless Downgrader is one of your current roles, you may only raise the classification of message files and text files.

2. *Show Permits* displays which commands others may invoke on the specified entity.

3. *Change Permits* enables you to allow or disallow others to invoke particular commands on the specified entity.

4. *Show User Information* displays a user's clearance, authorized roles (with current roles starred *), and terminal name. You must have SSO as a current role to show information about users other than yourself.

5. *Change User Role* allows you to modify your current roles.

6. *Change Password* replaces your old password with a new one of your choice. It requires that the current password first be entered correctly.

7. *Show Terminal Information* displays the maximum and the current screen classification of a specified terminal.

8. *Print Permits* is like Show Permits, except that the output is sent to the hard copy printer instead of the screen.

Security Officer Menu

1	2	3	4	5	6	7	8
CREATE New User	REMOVE User	CHANGE User Password	CHANGE User Clearance	CHANGE User Roles	CREATE New Terminal	REMOVE Terminal	CHANGE Terminal Classif

Note: these commands can only be invoked when SSO is one of your current roles.

1. *Create New User* creates a new user for authorized use of the MMS. This requires that a userid, clearance, password, and authorized role set be specified. The system then creates an message file directory, text file directory, and inbox for the new user.

2. *Remove User* removes a user from authorized use of the MMS and destroys the associated directories and any text files, message files, and messages that are solely in those directories.

3. *Change User Password* changes a user's password. Unlike the Change Password command of the Security Menu, the current password is not required.

4. *Change User Clearance* changes a user's clearance.

5. *Change User Roles* adds or removes a role from a user's authorized role set.

6. *Create New Terminal* adds a terminal to the list of terminals permitted to access the MMS.

7. *Remove Terminal* removes a terminal from the list of terminals permitted to access the MMS.

8. *Change Terminal Classification* raises or lowers the maximum screen classification for a specified terminal.

Function Key Overlays

The function keys on your terminal invoke special operations for selecting command menus and maintaining the display window. When you are working with the editor, these keys are redefined with specialised editing commands.

Most of the commands are self-explanatory, many are the same in both the message system and the editor. Each terminal type has its own overlay, so be sure to use the appropriate one.

Regent 40, Regent 60

M2 Function Keys

Use function keys for commands shown here on lower row
Use SHIFT + function keys for commands shown here on upper row
Use digit keys for commands shown on screen

	SCROLL LARGE BACK	SCROLL LARGE FWD	CLEAR WINDOW		Security Officer Menu		LOGOUT
ABORT	SCROLL SMALL BACK	SCROLL SMALL FWD	REDRAW SCREEN	Main Menu	Security Menu	Copy + Dup Menu	Sending Msgs. Menu
F1	F2	F3	F4	F5	F6	F7	F8

M2 Function Keys – in Message Editor

Use function keys for commands shown here on lower row
Use SHIFT + function keys for commands shown here on upper row
Use arrow keys to move cursor

Undo Command	SCROLL LARGE BACK	SCROLL LARGE FWD	Make New Parag.	Move Fwd Field	Move Back Word	Move Fwd Word	Finished Editing + Abort
ABORT	SCROLL SMALL BACK	SCROLL SMALL FWD	REDRAW SCREEN	Delete Char	Delete Word	Delete This Line	Finished Editing + Update
F1	F2	F3	F4	F5	F6	F7	F8

Freedom 220

M2 Function Keys

Use function keys for commands shown here on lower row
Use SHIFT + function keys for commands shown here on upper row
Use digit keys for commands shown on screen

	SCROLL LARGE BACK	SCROLL LARGE FWD	CLEAR WINDOW				Security Officer Menu		LOGOUT
ABORT	SCROLL SMALL BACK	SCROLL SMALL FWD	REDRAW SCREEN			Main Menu	Security Menu	Copy + Dup Menu	Sending Msgs. Menu
F1	F2	F3	F4	F5		F6	F7	F8	F9

M2 Function Keys – in Message Editor

Use function keys for commands shown here on lower row
Use SHIFT + function keys for commands shown here on upper row
Use arrow keys to move cursor

Undo Command	SCROLL LARGE BACK	SCROLL LARGE FWD	Make New Parag.			Move Fwd Field	Move Back Word	Move Fwd Word	Finished Editing + Abort
ABORT	SCROLL SMALL BACK	SCROLL SMALL FWD	REDRAW SCREEN			Delete Char	Delete Word	Delete This Line	Finished Editing + Update
F1	F2	F3	F4	F5		F6	F7	F8	F9

Editor Commands

Message Editor

The function key commands are given below. Most of them are self-explanatory, many are the same in the message system and in the editor.

M2 Function Keys – in Message Editor *Use function keys for commands shown here on lower row* *Use SHIFT + function keys for commands shown here on upper row* *Use arrow keys to move cursor*							
Undo Command	SCROLL LARGE BACK	SCROLL LARGE FWD	Make New Parag.	Move Fwd Field	Move Back Word	Move Fwd Word	Finished Editing + Abort
ABORT	SCROLL SMALL BACK	SCROLL SMALL FWD	REDRAW SCREEN	Delete Char	Delete Word	Delete This Line	Finished Editing + Update
F1	F2	F3	F4	F5	F6	F7	F8

Other Commands

CONTROL-A	*Move cursor to beginning of current line*
CONTROL-E	*Move cursor to end of current line*
ESCAPE-a	*Move cursor backward by one sentence*
ESCAPE-e	*Move cursor forward by one sentence*
ESCAPE-[	*Move cursor backward by one paragraph*
ESCAPE-]	*Move cursor forward by one paragraph*
ESCAPE-<	*Move cursor to beginning of message*
ESCAPE->	*Move cursor to end of message*
CONTROL-K	*Delete (kill) from cursor to end of current line, saving text in special buffer*
CONTROL-Y	*Insert (yank) text saved in special buffer*
CONTROL-S	*Search for a string, forward from the cursor position*
CONTROL-R	*Search for a string, backward from the cursor position*
ESCAPE-R	*Global replace one string with another*
ESCAPE-q	*Global replace one string with another, but ask individually whether each occurrence should be replaced*
ESCAPE-j	*Justify the current paragraph*
CONTROL-O	*Make a blank line above current line*
CONTROL-T	*Transpose the two characters immediately before the cursor*
ESCAPE-SHIFT-F2	*Scroll the header window backwards*
ESCAPE-SHIFT-F3	*Scroll the header window forward*
CONTROL-Q	*Quote next character (to insert a control or other special character into your text)*
CONTROL-X-CONTROL-I	*Insert the contents of a Unix file into your message*
ESCAPE-?	*Search KWIC index of all emacs commands*
ESCAPE-x	*Execute-extended-command (for hard-core emacs users only)*

The "Undo" key undoes the last command you gave, then asks if you want to undo the next-to-the-last, etc. Type a space to continue undoing or a carriage return to stop undoing.

All function keys have synonyms defined for terminals that don't have these keys, but they are less convenient to use. Function key N can also be entered as ESCAPE-N. The arrow keys can be entered as ESCAPE-U, D, L, and R, for up, down, left, and right.

Permissions Editor

The Permissions Editor is a limited version of the Message Editor. The only keys you need are the arrows for positioning the cursor, the scrolling function keys, the edit abort and update keys, and the space bar for turning permissions on or off.

Error Messages

This section provides additional explanation of error messages you may encounter in your use of the MMS. Most error messages are generated by the precondition checker. Once a syntactically correct command has been constructed using the menu interface, it is passed to the precondition checker, which determines whether or not the command can be executed. Both security constraints (is the message to be displayed classified at or below the level of the terminal screen?) and other operational constraints (does the requested message file exist?) are checked.

Two of the error messages are generated by the editor. Before a message is updated, it is checked for proper syntax and security hierarchy. The errors must be corrected before the text file or message can be updated.

The same error messages can be evoked by many different commands. The error messages are listed alphabetically below, along with an explanation of probable causes and remedies for special cases. Key words and abbreviations used in the messages are explained in the next section.

action_address_list_empty
No addressees were given to the Forward for Action command.

action_addressee_clearance_does_not_dominate_msg_classification
A for action *addressee is not cleared for this message. The message was forwarded to no one.*

addressee_does_not_have_releaser_role
A for release *addressee is not an authorized* releaser. *The message was forwarded to no one.*

cannot_append_paragraph_list_to_paragraph
The Subject *field or single paragraph text file can only contain a single paragraph. You attempted to append a paragraph list to it.*

cannot_remove_your_only_current_role
Each person must have at least one role current when logged in.

can_only_append_address_to_address
Paragraphs cannot be copied to address fields. Address message fields (To, Cc) can only contain addressees.

cc_field_addressee_clearance_does_not_dominate_msg_classification
One of the addressees in the Cc *field is not cleared to receive this message. The message was sent to no one. Edit the message appropriately.*

clearance_does_not_dominate_dir_classification
You are not cleared to print this directory.

clearance_does_not_dominate_entity_classification
You are not cleared to display or print the permissions on this entity.

clearance_does_not_dominate_msg_classification
You are not cleared to print or display this message.

clearance_does_not_dominate_msg_file_classification
You are not cleared to print a message file of this classification.

clearance_does_not_dominate_new_msg_file_classification

You cannot create or reclassify a message file above your clearance level.

clearance_does_not_dominate_new_terminal_classification
You cannot reclassify the terminal above your clearance level.

clearance_does_not_dominate_new_tfile_classification
You cannot reclassify or create a text file above your clearance level.

clearance_does_not_dominate_tfile_classification
You are not cleared to display or print this text file.

clearance_does_not_dominate_tfile_dir_classification
You are not cleared to print this directory.

container_clearance_required_for_msg_file
This file is CCR. You must be cleared at least to the level of this file to access any messages contained in it.

coordination_addressee_clearance_does_not_dominate_msg_classification
A for coordination *addressee is not cleared to receive this message. It was forwarded to no one.*

dir_classification_does_not_dominate_new_msg_file_classification
You cannot reclassify or create a message file at a level that is not less than or equal to that of the containing directory.

dir_classification_does_not_dominate_msg_file_classification
The classification of the duplicate message file must be less than or equal to that of the intended containing directory.

directory_does_not_exist
There is no directory with the specified name. Check the spelling.

downgrader_role_required
You must have downgrader *as one of your current roles to lower the classification on a text file or message file. Add* downgrader *as a current role (if authorized).*

field_classification_does_not_dominate_tfile_classification
The classification of the message field you are copying to must be greater than or equal to that of the text file you are copying from.

file_name_already_exists
There is already a file in this directory with the specified name. Choose a different name, or rename the existing file.

from_field_classification_does_not_dominate_reply_classification
The contents of the from *field of the source message is copied to the* to *field of the reply. The classification of the reply must be at least as high as the* from *field of the source.*

inbox_cannot_be_deleted
The message file "inbox" cannot be deleted.

inbox_cannot_be_downgraded

The message file "inbox" cannot be downgraded.

info_address_list_empty
No addressees were given to the Forward for Information command.

info_addressee_clearance_does_not_dominate_msg_classification
A for info *addressee is not cleared to receive this message. It was forwarded to no one.*

maximum_classification_does_not_dominate_new_terminal_classification
The terminal cannot be reclassified above its maximum level. Show terminal information to see the maximum classification.

msg_entry_already_deleted
This message entry has been deleted or moved. To remove the entry permanently, expunge the message file. To restore the entry, undelete it.

msg_entry_not_deleted
This entry cannot be undeleted because it has not been deleted or moved.

msg_file_classification_does_not_dominate_msg_classification
The classification of the duplicate or readdressed message is not less than or equal to that of the message file that is to contain it. Use a message file of higher classification.

msg_file_classification_does_not_dominate_new_msg_classification
The classification of the message to be created must be less than or equal to that of the message file that is to contain it. Use a message file of higher classification.

msg_file_classification_does_not_dominate_reply_classification
The classification of the reply message is not less than or equal to that of the message file that is to contain it. Use a message file of higher classification.

msg_must_be_formal_to_be_readdressed
Informal messages cannot be readdressed. Forward the message to the desired recipients. If authorized, you may forward this message for info.

new_msg_file_classification_does_not_dominate_msg_file_contents
A message file must be classified at least as high as the classification of its contents. To downgrade the file, first remove the messages that are above the desired classification.

new_tfile_classification_does_not_dominate_contents_classification
A text file must be classified at least as high as its highest paragraph. To downgrade the text file, remove or downgrade the paragraph first.

no_access_permitted
You do not have permission to perform the requested operation on the specified entity. If the requested operation specified more than one entity, you lack the necessary permission for at least one entity. If authorized, you may change the permissions.

no_forwarding_address_given

No addressees were given to the Forward for Coordination or Release command.

no_such_entity_exists

The reference made is to a non-existent directory, message file, text file or message. Specifying an incorrect message number or misspelled file name can Display the directory or message file for proper spelling and message number.

not_a_draft_message

Only draft messages can be sent or forwarded for release or coordination. A sent message can be forwarded for information or action, or readdressed.

not_a_sent_message

Only sent messages can be forwarded for information or action, or readdressed. A draft message can be sent or forwarded for release or coordination.

only_sso_can_display_other_users

You must have SSO as one of your current roles to display information about another person. Add SSO as a current role (if authorized).

password_not_valid

The password you typed is not correct. The password was not replaced.

Recheck Security Hierarchy

A message field or paragraph has been labeled with an inappropriate security level. The overall classification of the file or message must dominate the classification of all the contained paragraphs and fields. The cursor is positioned at the location of the security error.

release_addressee_clearance_does_not_dominate_msg_classification

A for release *addressee is not cleared to receive this message. It was forwarded to no one.*

releaser_role_required_to_send_formal_messages

You must have releaser *as one of your current roles to send a formal message. Add* releaser *as a current role (if authorized) or forward the message for release to an authorized* releaser.

roles_not_authorized

The role chosen is not in your authorized role set. Show user information for a list of authorized roles.

security_officer_role_required

You must have SSO as one of your current roles to perform this operation. Add SSO as a current role (if authorized).

syntax error line n

This error message can signal countless possible mistakes in the message or text file structure. The detected error occured n *lines down from the black bar. Common errors include:*

- *missing overall security level (this includes text typed after the text field label, but before a new paragraph label);*
- *modified message field identifiers;*
- *more than one paragraph in the subject field; and*
- *text in any of the address fields.*

subject_field_classification_does_not_dominate_reply_classification
The contents of the subject *field of the source message are copied to the* subject *field of the reply. The classification of the reply must be at least as high as the* subject *field of the source.*

target_tfile_classification_does_not_dominate_source_tfile_classification
The text file you are copying to must have a classification at least as high as that of the text file you are copying from.

terminal_already_exists
A terminal of the specified name already exists. It must be removed before a new terminal of this name can be created.

terminal_classification_does_not_dominate_msg_classification
In order to display, edit, or reply to a message, the screen classification must be at least as high as that of the specified message. Reclassify the screen to the appropriate level.

terminal_classification_does_not_dominate_new_msg_classification
The terminal screen classification must be at least as high as that of the message to be created. Reclassify the screen to the approporiate level.

terminal_classification_does_not_dominate_new_tfile_classification
The terminal screen classification must be at least as high as that of the text file to be created. Reclassify the screen to the appropriate level.

terminal_classification_does_not_dominate_tfile_classification
The terminal screen classification must be at least as high as that of the text file to be displayed or edited. Reclassify the screen to the appropriate level.

terminal_does_not_exist
No terminal with the specified name exists. Show terminal information. Check the spelling.

text_file_type_is_not_compatible
Only text files of the same type can be appended to each other. Text file types are paragraph, paragraph list, and address list. The To, From, *and* Cc *message fields can only contain an address list. The* Subject *field can only contain a paragrph. The* Text *field can contain a paragraph or a paragraph list.*

tfile_classification_does_not_dominate_field_classification
The classification of the text file must be at least as high as that of the message field to be copied.

tfile_dir_classification_does_not_dominate_new_tfile_classification
A text file cannot be created or reclassified to a level greater than that of the containing directory.

tfile_dir_classification_does_not_dominate_tfile_classification
The text file to be duplicated has a classification greater than that of the intended target directory. The directory cannot contain this file.

tfile_directory_does_not_exist

A directory of this name does not exist. Check the spelling.

to_field_addressee_clearance_does_not_dominate_msg_classification
One of the addressees in the To *field is not cleared to receive this message. It was sent to no one. Edit the message appropriately.*

to_field_empty
No addressees were given in the To *field of the message. It was sent to no one. Edit the message appropriately.*

user_already_exists
A user by that name is already authorized to use the MMS. Reassign the new user another name or remove the current user from the system.

user_does_not_exist
One or more of the addresses is not a valid userid. The message was not sent or forwarded. Check the spelling and capitalization. Userids contain no blanks or punctuation.

users_that_are_currently_logged_in_cannot_be_destroyed
An SSO cannot destroy a user who is logged in.

Key Words and Abbreviations

address
A userid denoting the person or organization to whom a message is to be sent or forwarded. In practice, an individual's last name, in lower case, is frequently used as his userid.

address list
A list of addresses separated by blanks. An address list can appear in a text file, a message field (To, Cc) and in Forward and Readdress commands.

dir
Directory.

directory
Either a message file directory or text file directory, depending on the context.

dominates
'Greater than or equal to' in the usual sense applied when comparing security levels. For example, Top Secret *dominates* Secret; Top Secret white *dominates* Top Secret; *but* Top Secret white *does not dominate* Top Secret red.

entity
A data structure in the MMS that has an explicit classification. Directories, files, messages, message fields, paragraph lists, paragraphs, and address lists are entities.

field
Message field.

file name
Either a message file name or text file name, depending on the context.

msg
Message.

msg file
Message file.

paragraph
An entity consisting of one security label and text.

paragraph list
An entity consisting of one overall security label and one or more paragraphs. Each paragraph in the list has its own security label. The overall security label must dominate that of each paragraph in the list.

tfile
A text file. An entity that can hold a single paragraph, paragraph list, or address list. The classification of the text file must dominate that of its contents.

Appendix A

The Secure MMS M2 Prototype Tourguide

This exercise serves as an introduction to the M2 rapid prototype of the Secure MMS project. The user interface of this prototype will help guide you through this exercise by prompting you for any needed information. However, there are a few things of which you should be aware before you start:

A. When typing security levels, just type a "T" for TOP SECRET to appear, "S" for SECRET, "C" for CONFIDENTIAL and "U" for UNCLASSIFIED (lower case t,s,c,u are also accepted). When compartment names follow, separate them only by blanks. No blank is needed preceding the first compartment.

B. The function keys are assigned certain tasks. You should have received a two-sided template describing these keys. One side gives the meaning of the function keys in the normal case; the second side describes the meaning of the function keys within the prototype's editor. Within the editor, the arrow keys can be used to move the cursor, and the backspace key deletes the current character.

C. Unless the prototype asks for the return key to be entered, it is not necessary to do so.

D. If you make a mistake while typing a command, you can use the ABORT key (see template) to cancel the current command. If the prototype detects that you have typed an erroneous key, it will ignore that keystroke and cause an audible *beep*.

The tour is set in the revolutionary war era; you will play the part of Benjamin Franklin.

Please complete the following tasks:

1. Login using

USER:	franklin
PASSWORD:	fireplace
SECURITY:	T white
ROLES:	user

2. Display each of the messages in Franklin's file inbox.
   What is the citation number of the message you cannot view? ____

3. Display the message file directory.

4. Move the message in inbox about Benedict Arnold's behavior to the message file called rumors.
   Note that inbox is classified at user's clearance level, but messages do not inherit this classification when moved to other files.

   Was the *move* successful? ____

5. Forward the same message for ACTION to washington (Hint: look at the *Sending Msgs* Menu).

6. Copy the message in inbox about Adams' delegation of work to the message file admin.
   Was the *copy* successful? ____

7. Create a FORMAL message with the security level of CONFIDENTIAL in the message file **admin** and enter some fields. (Don't forget to flip over your function key guide to the editor side.) Try entering things like a paragraph with a classification higher than the security level of the message.

8. Display the text file directory and any text files in it.

9. Copy the text file into the text field of the message you just created.

10. Print this draft formal message.

11. Send the formal message.
    Was the *send* successful? ____

12. Display the user information on franklin (Hint: look at the *Security* Menu).

13. Add the *releaser* role to your current set of roles.

14. Send the formal message.
    Was the *send* successful? ____

15. Raise the current classification of the terminal to **T red white**. Display your inbox.
    Is there anything new? ____

16. Reply to the message from adams with an INFORMAL message.

17. Logout (or continue to experiment as you wish).

Thank you for your assistance in this project.

Please write any comments or suggestions in the space below:

Appendix B

NRL Secure Military Message System Project Bibliography

Listed below are significant, externally distributed memoranda, papers, and reports produced as part of the NRL Secure Military Message Systems project. Copies may be obtained from the cited sources or by writing Code 7590, Naval Research Laboratory, Washington, D.C., 20375-5000, Attn: SMMS documents. Please specify the documents you wish and whether you would like to be included on the mailing list for future documents. For those unfamiliar with the project, Land82 and Heit85 are basic references. Corn84 documents the internal structure of the M2 rapid prototype.

Corn84 — Cornwell, M., and Jacob, R. J. K., "Structure of a Rapid Prototype Secure Military Message System," Proc. 7th DoD/NBS Computer Security Conference, Gaithersburg, MD, 24-26 Sept. 1984, pp.48-57.

Heit80 — Heitmeyer, C.L., and Wilson, S.H., "Military Message Systems: Current Status and Future Directions," IEEE Transactions on Communications, Vol. COM-28, No. 9, September 1980, pp.1645-1654.

Heit82 — Heitmeyer, C.L., Landwehr, C.E., and Cornwell, M., "The use of quick prototypes in the secure military message systems project," Proc. ACM SIGSOFT Second Software Engineering Symposium: Workshop on Rapid Prototyping, April, 1982, Columbia, MD. Reprinted in ACM SIGSOFT Software Engineering Notes, Vol. 7, No. 5 (Dec. 1982) pp. 85-87.

Heit84 — Heitmeyer, C.L., and Landwehr, C.E., "Designing secure message systems: the Military Message Systems (MMS) project," In Proc. IFIP 6.5 Working Conf. on Computer-Based Message Services, May 1984, Nottingham, England (proc. published by Elsevier, North Holland).

Heit85 — Heitmeyer, C.L., and Cornwell, M.R. "Specifications for three members of the Military Message System (MMS) family," NRL Memorandum Report 5645, Sept. 9, 1985.

Jaco83a — Jacob, R.J.K., "Using formal specifications in the design of a human-computer interface," Comm. ACM Vol. 26 pp. 259-264 (1983). (also appeared Proc. Human Factors in Computer Systems Conference, pp. 315-321 (1982),).

Jaco83b — Jacob, R.J.K., "Formal specification of the user interface of a receive-only SMMS prototype," NRL Technical Memorandum 7590-203:RJ:rj, 11 August 1983.

Jaco83c — Jacob, R.J.K., "Executable specifications for a human-computer interface," Proc. Human Factors in Computer Systems Conference, (1983), p.28-34.

Jaco84 Jacob, R.J.K., "Designing a human-computer interface with software specification techniques" Proc. Second Symposium on Empirical Foundations of Information and Software Sciences, Atlanta, Ga., 1984.

Jaco85a Jacob, R.J.K., "An executable specification technique for describing human-computer interaction," in Advances in Human-Computer Interaction, ed. H.R. Hartson, Ablex Publishing Co., Norwood, N.J. (1985), pp.211-242.

Jaco85b Jacob, R.J.K., "A State Transition Diagram Language for Visual Programming," IEEE Computer, Vol. 18(8) (August 1985) pp. 51-59.

Land80 Landwehr, C.E., "Assertions for verification of multi-level secure military message systems," Workshop on Formal Verification, SRI, Menlo Park, CA, April 1980. Reprinted in ACM SIGSOFT Software Engineering Notes, Vol. 5, No. 3 (July 1980) pp.46-47.

Land82a Landwehr, C.E., "What security levels are for and why integrity levels are unnecessary," NRL Technical Memorandum 7590-308:CL:uni, 23 February 1982.

Land82b Landwehr, C.E., and Heitmeyer, C.L., "Secure military message systems: requirements and security model," NRL Memorandum Report 4925, Sept. 1982. ADA119960

Land83 Landwehr, C.E., "The best available technologies for computer security," IEEE COMPUTER, July 1983, pp.86-100.

Land84a Landwehr, C.E., and Carroll, J. "Hardware requirements for secure computer systems: a framework," Proc. IEEE 1984 Symposium on Security and Privacy, pp. 34-40.

Land84b Landwehr, C.E., Heitmeyer, C.L., and McLean, J., "A security model for military message systems," ACM Trans. on Computer Systems, August, 1984. Also published as NRL Report 8806, May 31, 1984. ADA142355

Land85 Landwehr, C.E., "Some lessons from formalizing a security model," Proceedings VERkshop III, February, 1985, reprinted in ACM SIGSOFT Software Engineering Notes, August, 1985.

McLe84 McLean, J., Landwehr, C., and Heitmeyer, C.L., "Formalising the MMS security model," Proc. 1984 IEEE Symp. on Sec. and Priv., Oakland, CA.

McLe85 McLean, J., "A comment on the 'Basic Security Theorem' of Bell and LaPadula," Information Processing Letters 20 (1985) 15 February 1985, pp.67-70.

END

FILMED

5-86

DTIC